

REMARKS

In the current and final Office Action, claims 1-47 were examined.

Claims 1-47 were rejected.

Specifically:

Claims 1-2, 4-11, 13-28, 30-31, 33-35, and 37-42 were “rejected under 35 U.S.C. 102(e) as being anticipated by Downs et al (US 6,574,609).”

Claims 3, 12, 29, 32, 36, and 43-47 were “rejected under 35 U.S.C. 103(a) as being unpatentable over Downs et al. (US 6,574,609) as applied to claims 1-2, 4-11, 13-28, 30-31, 33-35, and 37-42 above, and further in view of Yoshida et al. (US 6,674,874).

1 I. It is respectfully submitted that no art of record (including Downs et
2 al. and/or Yoshida et al.), either alone or in any combination, anticipates or renders
3 obvious claims 1-43.

4
5 A. For example, (i) the secure container (SC) of Downs et al.
6 includes usage conditions, and (ii) the license and/or certificate of Downs et
7 al. does not include usage conditions.

8
9 1. Downs et al. reads at column 15, lines 21-24, in
10 pertinent part:

11 “And Usage Conditions 206 for content licensing management as
12 described below. *The SC(s) 200 comprises Usage Conditions 206...*”

13 (emphasis added)

14
15 2. Downs et al. reads at column 11, line 64 to column 12,
16 line 9, in pertinent part:

17 “The End-User Device(s) 109 manages the download and storage
18 of the SCs containing the Digital Content; requests and manages receipt of
19 the encrypted Digital Content keys from the Clearinghouse(s) 105;
20 processes the watermark(s) every time the Digital Content is copied or
21 played; manages the number of copies made (or deletion of the copy) in
22 accordance with the Digital Content's Usage Conditions; and performs the
23 copy to an external media or portable consumer device if permitted. The
24 portable consumer device can perform a subset of the End-User Player
25 Application 195 functions *in order to process the content's Usage*
Conditions embedded in the watermark.”

(emphasis added)

1 3. Downs et al. reads at column 14, lines 41-49, in
2 pertinent part:

3 “A digital certificate is used to authenticate or verify the identity
4 of a person or entity that has sent a digitally signed message. A certificate
5 is a digital document issued by a certification authority that binds a public
6 key to a person or entity. The certificate includes the public key, the name
7 of the person or entity, an expiration date, the name of the certification
8 authority, and other information. The certificate also contains the digital
9 signature of the certification authority.”

10 4. Downs et al. reads at column 28, line 63 to column 29,
11 line 12, in pertinent part:

12 “Clearinghouse(s) Certificate(s)--A certificate from a certification
13 authority or from the Clearinghouse(s) 105 that contains the signed Public
14 Key 621 of the Clearinghouse(s) 105. There may be more than one
15 certificate, in which case a hierarchical level structure is used with the
16 highest level certificate containing the public key to open the next lowest
17 level certificate is reached which contains the Public Key 621 of the
18 Clearinghouse(s) 105.

19 Certificate(s)--A certificate from a certification authority or from
20 the Clearinghouse(s) 105 that contains the signed Public Key 621 of the
21 entity that created the SC(s). There may be more than one certificate, in
22 which case a hierarchical level structure is used with the highest level
23 certificate containing the public key to open the next level certificate, and
24 so on, until the lowest level certificate is reached which contains the public
25 key of the SC(s) creator.”

26 5. Downs et al. reads at column 11, lines 18-24, in
27 pertinent part:

28 “Once these verifications are satisfied, the Clearinghouse(s) 105
29 sends the decryption key for the Content 113 to the requesting End-User(s)

1 packed in a License SC. The key is encrypted in a manner so that only the
2 authorized user can retrieve it. If the End-User's request is not verifiable,
3 complete, or authorized, the Clearinghouse(s) 105 repudiates the request
4 for the decryption key.”

5 6. Downs et al. reads at column 28, lines 14-16, in
6 pertinent part:

7 “Usage Conditions--A part that contains information that
8 describes usage options, rules, and restrictions to be imposed on an End-
9 User(s) for use of the Content 113.”

10 7. Downs et al. reads at column 9, lines 51-62, in pertinent
11 part:

12 “A Metadata Assimilation and Entry Tool 161 is used to extract
13 metadata from the Content Provider(s)' Database 160 (for a music example
14 the Content 113 information such as CD title, artist name, song title, CD
15 artwork, and more) and to package it for electronic distribution. *The*
16 *Metadata Assimilation and Entry Tool 161 is also used to enter the Usage*
17 *Conditions for the Content 113.* The data in Usage Conditions can include
18 copy restriction rules, the wholesale price, and any business rules deemed
19 necessary. A Watermarking Tool is used to hide data in the Content 113
20 that identifies the content owner, the processing date, and other relevant
21 data.”

22 (emphasis added)

23 8. Downs et al. reads at column 8, lines 13-29, in pertinent
24 part:

25 “Digital watermarking also provides the means to identify the
origin of authorized or unauthorized copies of Content. An initial
watermark in the Content is embedded by the content proprietor to identify

1 the content proprietor, specify copyright information, define geographic
2 distribution areas, and add other pertinent information. A second
3 watermark is embedded in the Content at the End-User Device(s) to
4 identify the content purchaser (or licensee) and End-User Device(s),
5 specify the purchase or license conditions and date, and add any other
6 pertinent information.

7 Since watermarks become an integral part of the Content, they are
8 carried in the copies independent of whether the copies were authorized or
9 not. *Thus the Digital Content always contains information regarding its
10 source and its permitted use regardless of where the content resides or
11 where it comes from.* This information may be used to combat illegal use
12 of the Content.”

13 (emphasis added)

14 B. Thus, no art of record, either alone or in any combination,
15 anticipates or renders obvious at least the following elements in conjunction
16 with the other elements of their respective claims:

17 **Claim 1: an authentication module configured to access a certificate,**
18 **which indicates permissible uses of the digital content file,**
19 **associated with and separate from the digital content file**

20 **Claim 11: associating the digital content file with a certificate that**
21 **contains copyright information including at least one**
22 **indication regarding a permissible use of the digital content file**
23 **and is not a part of the digital content file.**

24 **Claim 17: configuring the certificate file with permissible use**
25 **information about the digital content file so that when the**
digital content file is processed, the digital content file is

1 processed in accordance with the permissible use information
2 contained in the certificate file.

3 Claim 25: if the watermark signal is detected, attempting to locate a
4 certificate associated with the digital content file, the certificate
5 including copyright information having at least one indication
6 regarding a permissible use of the digital content file.

7 Claim 30: the certificate containing copyright information including
8 at least one indication regarding a permissible use of the digital
9 content file.

10 Claim 35: if the watermark is detected, attempting to locate a
11 certificate that is associated with the digital content file, the
12 certificate containing instructions regarding the digital content
13 file . . . wherein the watermark only indicates the existence of
14 the certificate.

15 Claim 43: wherein the 1-bit watermark indicates the presence of a
16 certificate associated with the digital content, the certificate
17 containing copyright information including at least one
18 indication regarding a permissible use of the digital content
19 and being stored apart from the digital content.
20
21
22
23
24
25

1 Reasons for the allowability of independent claims 1, 11, 17, 25, 30, 35, and
2 43 have been provided above. Claims 2-10, 12-16, 18-24, 26-29, 31-34, 36-42, and
3 44-47 depend from these independent claims 1, 11, 17, 25, 30, 35, and 43,
4 respectively. Although each also includes additional element(s) militating toward
5 allowability, it is respectfully submitted that these dependent claims are allowable at
6 least for the reasons given above in connection with their respective independent
7 claims.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

By: Keith W. Saunders
Keith W. Saunders
Reg. No. 41,462
(509) 324-9256 x238